(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－240687

(43)公開日　平成10年(1998)９月11日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ
	３１０		３１０Ｄ
1/00	３７０	1/00	３７０Ｅ
13/00	３５１	13/00	３５１Ｍ

審査請求　未請求　請求項の数３　ＯＬ　（全８頁）

(21)出願番号　特願平9－46739

(22)出願日　平成９年(1997)２月28日

(71)出願人　000003562
株式会社テック
静岡県田方郡大仁町大仁570番地

(72)発明者　大國　裕二
静岡県三島市南町６番78号　株式会社テック三島工場内

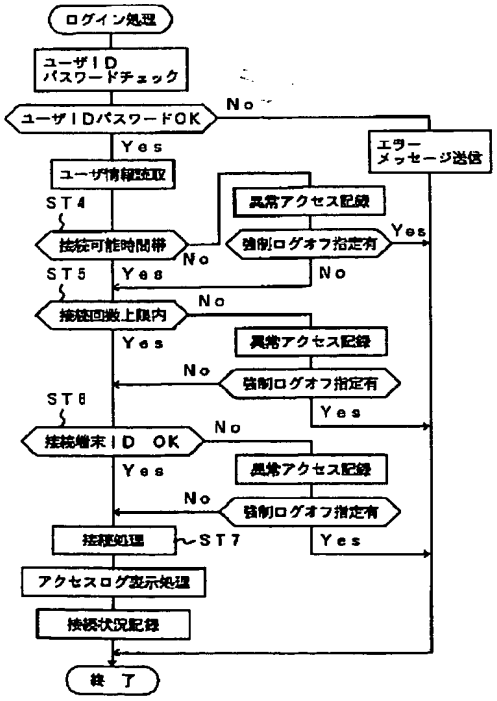
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　ネットワークシステム

(57)【要約】

【課題】不正アクセスを防止すると共に検出して、不正アクセス検出におけるユーザの負担を軽減する。

【解決手段】ネットワークを管理するサーバ２に各ユーザ毎に接続条件（接続時間上限、接続可能時間帯、接続可能曜日帯、接続回数上限及び接続端末ＩＤ）を登録したユーザ別情報ファイル１２と、各ユーザ毎にアクセスした接続状況を示すアクセスログファイルを履歴的に記憶するユーザ別アクセスログファイル１３とを設け、接続条件を満たさないアクセスについてはアクセスログファイルに異常アクセスを記録し、ログインしたクライアントに対して履歴的にアクセスログファイルを送信して表示させるもの。



1

【特許請求の範囲】
【請求項１】　ネットワークに接続された複数のデータ処理装置からなるネットワークシステムにおいて、
前記各データ処理装置毎に前記ネットワークへの接続条件データを記憶した接続条件データ記憶手段と、
前記データ処理装置がパスワード又は識別番号により前記ネットワークへの接続を要求したときに、前記接続条件データ記憶手段に記憶された該当する接続条件データに基づいて、前記データ処理装置の前記ネットワークへの接続を制御するネットワーク接続制御手段とを設けたことを特徴とするネットワークシステム。
【請求項２】　ネットワークに接続された複数のデータ処理装置からなるネットワークシステムにおいて、
前記各データ処理装置毎に前記ネットワークへの接続条件データを記憶した接続条件データ記憶手段と、
前記データ処理装置がパスワード又は識別番号により前記ネットワークへの接続を要求したときに、前記接続条件データ記憶手段に記憶された該当する接続条件データに基づいて、前記データ処理装置の前記ネットワークへの接続を制御するネットワーク接続制御手段と、
前記データ処理装置の前記ネットワークへの接続が、前記接続条件データ記憶手段に記憶された該当する接続条件データに対して異常か否かを判断する接続異常判断手段と、
この接続異常判断手段により前記データ処理装置の前記ネットワークへの接続が異常と判断された後で、この異常の発生を示すデータを前記データ処理装置へ送信する異常発生データ送信手段とを設けたことを特徴とするネットワークシステム。
【請求項３】　ネットワークに接続された複数のデータ処理装置からなるネットワークシステムにおいて、
前記各データ処理装置毎に前記ネットワークへの接続条件データを記憶した接続条件データ記憶手段と、
前記データ処理装置がパスワード又は識別番号により前記ネットワークへの接続を要求したときに、前記接続条件データ記憶手段に記憶された該当する接続条件データに基づいて、前記データ処理装置の前記ネットワークへの接続を制御するネットワーク接続制御手段と、
前記データ処理装置の前記ネットワークへの接続が、前記接続条件データ記憶手段に記憶された該当する接続条件データに対して異常か否かを判断する接続異常判断手段と、
所定期間内の前記データ処理装置の前記ネットワークへの接続結果データからなる接続履歴データを送信する接続履歴データ送信手段とを設け、
前記接続異常判断手段により異常と判断された接続があったときには、この異常と判断された接続結果データを正常の接続結果データと識別できるように処理して前記接続履歴データに含ませたことを特徴とするネットワークシステム。

2

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、ネットワーク及びこのネットワークに接続された複数のデータ処理装置からなるネットワークシステムに関する。
【０００２】
【従来の技術】公衆回線における各種のネットワークやＬＡＮ(local area network)等の専用のネットワークに対して、端末装置(パーソナルコンピュータやマルチメディア装置)を接続して、ネットワークを利用して情報サービスや通信サービスを受けることが広く普及している。このようなネットワークでは、ネットワークを管理し、情報サービスや通信サービスを供給するサーバ(サーバマシン)と、ネットワークにアクセスして情報サービスや通信サービスを受けるクライアント(クライアントマシン)とによりネットワークシステムが形成される。ユーザは、このクライアントを使用することによりこのネットワークシステムを利用することができる。
【０００３】ユーザは、予め情報サービスや通信サービスを受けるために、契約によってサーバに対して登録し、このサーバにより管理されるネットワークに対してアクセスするためのユーザＩＤ、マスタパスワード及びサブパスワードを取得する。すなわち、このサーバにより管理されるネットワークにアクセス(ログイン)するためには、ユーザが使用するクライアントからユーザＩＤ、マスタパスワード及びサブパスワードを正確に入力してサーバの認証を受けなければならないようになっている。もし、ユーザＩＤ、マスタパスワード及びサブパスワードを間違って入力すると、サーバが未契約者としてこのネットワークへのアクセスを禁止し、情報サービスや通信サービスを受けられないことになる。また、サーバはユーザに対して、前回の接続開始日時、終了日時及び接続時間について通知するサービスを行うものも知られている。
【０００４】
【発明が解決しようとする課題】しかし、ユーザＩＤやパスワード等は契約した利用者の不注意等の原因によって盗用され、契約した利用者以外の者による不正アクセスが行われる可能性がある。このような不正アクセスは、サーバ及びクライアントに対して損害を与え、ネットワークシステムの信頼性を低下させるので、不正アクセスの検出が必要であるが、サーバはユーザ(契約した利用者)を判断するのに、ユーザＩＤやパスワードしか使用していないので、ユーザＩＤやパスワードの盗用による不正アクセスは検出することができないという問題があった。サーバからの前回の接続開始日時、終了日時及び接続時間の通知によって、ユーザ自身で不正アクセスを検出することも可能であるが、ユーザに常にアクセス状況の確認が求められ、不正アクセス検出におけるユーザの負担が大きいという問題があった。

【０００５】そこでこの発明は、不正アクセスを防止すると共に検出することができ、不正アクセス検出におけるユーザの負担を軽減することができるネットワークシステムを提供することを目的とする。

【０００６】

【課題を解決するための手段】請求項１対応の発明は、ネットワークに接続された複数のデータ処理装置からなるネットワークシステムにおいて、各データ処理装置毎にネットワークへの接続条件データを記憶した接続条件データ記憶手段と、データ処理装置がパスワード又は識別番号によりネットワークへの接続を要求したときに、接続条件データ記憶手段に記憶された該当する接続条件データに基づいて、データ処理装置のネットワークへの接続を制御するネットワーク接続制御手段とを設けたものである。

【０００７】請求項２対応の発明は、ネットワークに接続された複数のデータ処理装置からなるネットワークシステムにおいて、各データ処理装置毎にネットワークへの接続条件データを記憶した接続条件データ記憶手段と、データ処理装置がパスワード又は識別番号によりネットワークへの接続を要求したときに、接続条件データ記憶手段に記憶された該当する接続条件データに基づいて、データ処理装置のネットワークへの接続を制御するネットワーク接続制御手段と、データ処理装置のネットワークへの接続が、接続条件データ記憶手段に記憶された該当する接続条件データに対して異常か否かを判断する接続異常判断手段と、この接続異常判断手段によりデータ処理装置のネットワークへの接続が異常と判断された後で、この異常の発生を示すデータをデータ処理装置へ送信する異常発生データ送信手段とを設けたものである。

【０００８】請求項３対応の発明は、ネットワークに接続された複数のデータ処理装置からなるネットワークシステムにおいて、各データ処理装置毎にネットワークへの接続条件データを記憶した接続条件データ記憶手段と、データ処理装置がパスワード又は識別番号によりネットワークへの接続を要求したときに、接続条件データ記憶手段に記憶された該当する接続条件データに基づいて、データ処理装置のネットワークへの接続を制御するネットワーク接続制御手段と、データ処理装置のネットワークへの接続が、接続条件データ記憶手段に記憶された該当する接続条件データに対して異常か否かを判断する接続異常判断手段と、所定期間内のデータ処理装置のネットワークへの接続結果データからなる接続履歴データを送信する接続履歴データ送信手段とを設け、接続異常判断手段により異常と判断された接続があったときには、この異常と判断された接続結果データを正常の接続結果データと識別できるように処理して接続履歴データに含ませたものである。

【０００９】

【発明の実施の形態】以下、この発明の実施の形態を図面を参照して説明する。図１は、この発明を適用したネットワークシステムの要部構成を示すブロック図である。回線（ネットワーク）１には、ネットワークを管理するデータ処理装置としてのサーバ（サーバマシン、例えばスーパーコンピュータ）２と、このサーバ２により管理するネットワークから情報サービス及び通信サービスを受けることが可能なように複数台のデータ処理装置としてのクライアント（クライアントマシン、例えばパーソナルコンピュータ）、すなわち第１のクライアント３-1と、第２のクライアント３-2と、…、第Ｎのクライアント３-Ｎとがそれぞれ接続されている。

【００１０】図２は、このネットワークシステムにおける前記サーバ２の前記各クライアント３-1～３-Ｎに対するログオン及びログオフ制御に関する要部機能構成を示すブロック図である。中央制御部１１は、図示しないが、制御部本体を構成するＣＰＵ(centralprocessing unit)、ＲＯＭ(read only memory)、ＲＡＭ(random access memory)等から構成されており、後述する各ブロックを制御する。

【００１１】ユーザ別情報ファイル１２には、接続条件データ記憶手段として、図３に示すユーザ別情報ファイルのフォーマットのように、各ユーザ毎に、ユーザＩＤ（識別番号）、マスタパスワード、サブパスワード、接続条件として接続時間上限、接続可能時間帯、接続可能曜日帯、接続回数上限、接続端末ＩＤ、さらに接続状況として接続開始年月日、接続開始時間、接続終了年月日、接続終了時間、接続時間、接続回数のデータが記憶（設定・登録）されるようになっている。なお、接続端末ＩＤには、クライアントの端末ＩＤ（端末番号）を１台分でも複数台分でも登録することができる。また、ユーザ別アクセスログファイル１３には、図４に示すユーザ別アクセスログファイル（ログレコード）のフォーマットのように、各ユーザ毎に、ユーザＩＤ、接続開始年月日、接続開始時間、接続終了年月日、接続終了時間、接続端末ＩＤ、アクセスステータスのデータが履歴的に記憶される。

【００１２】ファイル制御部１４は、前記ユーザ別情報ファイル１２及び前記ユーザ別アクセスログファイル１３に対してファイルの書込み及び読取りを行う。アクセス制御部１５は、前記ファイル制御部１４により前記ユーザ別情報ファイル１２から読取った該当するユーザの接続条件のデータに基づいて、該当する（ユーザが使用している）クライアント３-xに対してログイン（ネットワークへの接続）及びログオフ（ネットワークからの切断）を制御するようになっている。

【００１３】アクセス監視部１６は、時計機能及びカレンダ機能を備え、前記アクセス制御部１５によりログイン制御されたクライアントを使用している各ユーザ毎に、ネットワークへの接続開始年月日時間（ログインと

なった年月日時間)及び終了年月日時間(ログオフとなった年月日時間)を記録(監視)するようになっている。　通知部１７は、クライアント３-xからログイン要求で入力したユーザＩＤ、マスタパスワード、サブパスワードが照合しない(誤りがある)ときに、エラーメッセージを該当するクライアント３-xへ送信すると共に、前記アクセス制御部１５によりログイン制御されたクライアントの各ユーザに対して、該当するユーザの(ユーザＩＤの)アクセスログファイル(ログレコード)を送信する。

【００１４】図５は、前記各クライアント３-1～３-Nがそれぞれ行うメイン処理の流れを示す図である。まず、ステップ１(ＳＴ１)の処理として、ユーザがキーボード等により入力したユーザＩＤ、マスタパスワード及びサブパスワードをサーバ２へ送信してログイン要求を行うログイン要求処理を行い、このログイン要求処理を終了すると、サーバ２からエラーメッセージを受信したか否かを判断する。ここで、エラーメッセージを受信したと判断すると、このエラーメッセージをディスプレイ等に表示し、このメイン処理を終了するようになっている。なお、このエラーメッセージを表示した後、もう再度(予め設定された回数だけ)、ステップ１のログイン要求処理をやり直すリトライ機能を備えても良いものである。

【００１５】また、エラーメッセージは受信しないと判断すると、サーバ２から送信されるアクセスしたユーザＩＤに関するログレコード(アクセスログファイル)を受信して、この受信したログレコード(アクセスログファイルの一覧)を表示するアクセスログ表示を行う。このとき、ステップ２(ＳＴ２)の処理として、接続条件(接続時間上限、接続可能時間帯、接続可能曜日帯、接続回数上限、接続端末ＩＤ)を登録・変更を行うための特殊操作が有るか否かを判断する。ここで、特殊操作はないと判断すると、後述するステップ３(ＳＴ３)の処理平行するようになっている。

【００１６】また、特殊操作が有ると判断すると、ユーザ(操作者)のマスタパスワードの入力を要求し、入力されたマスタパスワードの照合を行うマスタパスワード入力チェック処理を行う。このマスタパスワード入力チェック処理を終了すると、チェック結果によりマスタパスワードの照合が不一致でエラーとなったか否かを判断する。ここで、エラーとなったと判断すると、再び前述のステップ２の処理へ戻るようになっている。

【００１７】また、マスタパスワードの照合が一致し、エラーとならなかったと判断すると、ユーザ(操作者)の入力操作に基づいて、接続条件の各種データ(接続時間上限、接続可能時間帯、接続可能曜日帯、接続回数上限、接続端末ＩＤ)に関して登録・変更を行う接続条件登録処理を行い、この接続条件登録処理を終了すると、次のステップ３の処理へ移行するようになっている。ステップ３の処理は、情報サービス又は通信サービスを受ける業務処理を行い、この業務処理を終了すると、サーバに対してログオフ要求を送信して、ネットワークへの接続が切断されたことを確認するログオフ要求処理を行い、このログオフ要求処理を終了すると、このメイン処理を終了するようになっている。

【００１８】図６は、前記サーバ２が、前記クライアント３-xからログイン要求を受信したときに行うログイン処理(ネットワーク接続制御手段)の流れを示す図である。まず、クライアント３-xから送信されたユーザＩＤ、マスタパスワード及びサブパスワードを受信して、ユーザＩＤ、マスタパスワード及びサブパスワードについて照合するユーザＩＤ・パスワードチェックを行う。このユーザＩＤ・パスワードチェックチェックを終了すると、そのチェック結果によりユーザＩＤ、マスタパスワード及びサブパスワードの全て照合が一致した(ＯＫ)か否かを判断する。ここで、ユーザＩＤ、マスタパスワード及びサブパスワードのいずれか１つでも照合が一致しなかった(ＯＫではない)と判断すると、エラーメッセージをログイン要求の送信元のクライアントへ送信して、このログイン処理を終了するようになっている。

【００１９】また、ユーザＩＤ、マスタパスワード及びサブパスワードの全ての照合が一致した(ＯＫ)と判断すると、ユーザ別情報ファイルから該当するユーザＩＤに関する接続条件(接続時間上限、接続可能時間帯、接続可能曜日帯、接続回数上限、接続端末ＩＤ)及び接続状況(接続開始年月日、接続開始時間、接続終了年月日、接続終了時間、接続状況、接続回数)のデータを読取り、ステップ４(ＳＴ４)の処理として、今回のログイン要求の曜日及び時間に関して接続可能曜日帯及び接続可能時間帯の条件を満たしているか否かを判断する(接続異常判断手段)。

【００２０】ここで、今回のログイン要求が接続可能曜日帯及び接続可能時間帯の条件を満たしていないと判断すると、今回の該当するユーザのログイン要求に対して作成されるアクセスログファイルの接続開始時間に対するアクセスステータスとして異常アクセスを記録し、ソフトウエア的なフラグ又はハードウエア的なディップスイッチ等により接続可能時間外に関する強制ログオフの指定が有るか否かを判断する。ここで、強制ログオフの指定が有ると判断すると、このログイン処理を終了するようになっている。また、強制ログオフの指定がないと判断すると、後述するステップ５(ＳＴ５)の処理へ移行するようになっている。

【００２１】前述のステップ４の処理で、今回のログイン要求が接続可能曜日帯及び接続可能時間帯の条件を満たしていると判断すると、次のステップ５の処理へ移行するようになっている。ステップ５の処理は、読取った接続状況の接続回数のデータに＋１加算して、今回のログイン要求の接続回数が接続回数上限の条件を満たして

いる(接続回数上限内)か否かを判断する(接続異常判断手段)。

【００２２】ここで、今回のログイン要求が接続回数上限の条件を満たしていないと判断すると、今回の該当するユーザのログイン要求に対して作成されるアクセスログファイルの接続回数に対するアクセスステータスとして異常アクセスを記録し、接続回数上限オーバーに関する強制ログオフの指定が有るか否かを判断する。ここで、強制ログオフの指定が有ると判断すると、このログイン処理を終了するようになっている。また、強制ログオフの指定がないと判断すると、後述するステップ６(ＳＴ６)の処理へ移行するようになっている。

【００２３】前述のステップ５の処理で、今回のログイン要求が接続回数上限の条件を満たしていると判断すると、次のステップ６の処理へ移行するようになっている。ステップ６の処理は、ログイン要求の送信元のクライアント３-xの端末ＩＤ(端末番号)と接続条件データの接続端末ＩＤとを照合して一致するか否かを判断する(接続異常判断手段)。ここで、今回のログイン要求の送信元のクライアント３-xの端末ＩＤと接続条件データの接続端末ＩＤとが一致しないと判断すると、今回の該当するユーザのログイン要求に対して作成されるアクセスログファイルの端末ＩＤ(端末番号)に対するアクセスステータスとして異常アクセスを記録し、接続端末ＩＤ不一致に関する強制ログオフの指定が有るか否かを判断する。ここで、強制ログオフの指定が有ると判断すると、このログイン処理を終了するようになっている。また、強制ログオフの指定がないと判断すると、後述するステップ７(ＳＴ７)の処理へ移行するようになっている。

【００２４】前述のステップ６の処理で、ログイン要求の送信元のクライアント３-xの端末ＩＤと接続条件データの接続端末ＩＤとが一致したと判断すると、次のステップ７の処理へ移行するようになっている。

【００２５】ステップ７の処理は、ログイン要求の送信元のクライアント３-xをネットワークに接続させて、情報サービス又は通信サービスを受けれる状態にする接続処理を行い、ユーザ別アクセスログファイル１３から該当するユーザの過去の所定期間内の全てのアクセスログファイル(ログレコード)をログイン要求の送信元のクライアントへ送信してアクセスログ表示を指示するアクセスログ表示処理を行う(異常発生データ送信手段、接続履歴データ送信手段)。このアクセスログ表示処理を終了すると、ユーザ別情報ファイル１２の接続状況の接続開始年月日、接続開始時間及び接続回数にそれぞれデータを記録(書込み又は＋１加算更新処理)すると共に、アクセスログファイルの接続開始年月日、接続開始時間、接続端末ＩＤ及び必要な場合にはアクセスステータスにそれぞれデータを記録(作成)する接続状況記録を行う。この接続状況記録を終了すると、このログイン処理を終了するようになっている。この後、サーバ２は、ネットワークに接続したクライアントに応対して、情報サービス及び通信サービスを供給する処理を行うようになっている。

【００２６】図７は、前記サーバ２が、ネットワークに接続したクライアントに応対して、情報サービス及び通信サービスを供給する処理を行っている間に、定期的又はログオフ要求を受信した時に行うログオフ処理(ネットワーク接続制御手段)の流れを示す図である。まず、ステップ８(ＳＴ８)の処理として、接続している該当するクライアント３-xから送信されたログオフ要求が有る(を受信した)か否かを判断する。ここで、ログオフ要求が有ると判断すると、ステップ９(ＳＴ９)の処理として、該当するクライアント３-xに対してネットワークへの接続を切断する切断処理を行い、この切断処理を終了すると、ユーザ別情報ファイル１２の接続状況の接続終了年月日及び接続終了時間にそれぞれデータを記録すると共に、アクセスログファイルの接続時間及び必要な場合にはアクセスステータスにそれぞれデータを記録(作成)する接続状況記録を行う。この接続状況記録を終了すると、作成されたアクセスログファイルを完成して、ユーザ別アクセスログファイル１３に書込むログレコード作成を行い、このログレコード作成を終了すると、このログオフ処理を終了するようになっている。

【００２７】また、ステップ８の処理で、ログオフ要求はない(を受信していない)と判断すると、ユーザ別情報ファイル１２の接続状況の接続終了年月日及び接続終了時間にそれぞれデータを記録する接続状況記録を行い、ステップ１０(ＳＴ１０)の処理として、今回の接続状況(ユーザ別情報ファイル１２の接続終了時間から接続開始時間を減算して得られる接続時間)が接続条件データの接続時間上限の条件を満たしている(接続時間上限内)か否かを判断する(接続異常判断手段)。

【００２８】ここで、今回の接続状況が接続時間上限の条件を満たしていると判断すると、このログオフ処理を終了するようになっている。また、今回の接続状況が接続時間上限の条件を満たしていないと判断すると、今回の該当するユーザのログイン要求に対して作成されるアクセスログファイルの接続時間に対するアクセスステータスとして異常アクセスを記録し、接続時間上限オーバーに関する強制ログオフの指定が有るか否かを判断する。

【００２９】ここで、強制ログオフの指定が有ると判断すると、前述のステップ９の処理へ移行するようになっている。また、強制ログオフの指定がないと判断すると、このログオフ処理を終了するようになっている。

【００３０】このような構成のこの実施の形態において、各ユーザはサーバ２に対して、ＩＤにより接続条件として、接続時間上限、接続可能時間帯、接続可能曜日帯、接続回数上限及び接続端末ＩＤを予め登録しておく

ことができる。サーバ２は、ユーザＩＤ、マスタパスワード及びサブパスワードでログイン要求したユーザに対して、その接続条件として登録された接続可能曜日帯以外の場合、接続可能時間帯以外の場合、接続回数上限を越えた場合、接続端末ＩＤ以外のクライアントの使用の場合に対して、アクセスステータスとして異常アクセスをアクセスログファイルに記録する。従って、ユーザが通常アクセスしない時間帯にアクセスしたものをチェックする。また、ユーザが通常アクセスしない曜日にアクセスしたものをチェックする。また、ユーザが所定の期間内に通常アクセスしない回数アクセスしたときチェックする。また、ユーザが通常使用しないクライアントからアクセスしたものをチェックする。

【００３１】このとき、各接続条件について強制ログオフを指定していれば、ログイン要求は無視されて、ログイン要求の送信元のクライアント３-xはネットワークへ接続されないことになる。強制ログオフを指定しなければ、異常アクセスとして記録されるものの、クライアント３-xのネットワークへ接続は許可される。ログイン要求によりクライアント３-xがネットワークに接続されると、サーバからクライアント３-xへアクセスログファイル(ログレコード)が送信され、クライアント３-xにそのユーザのユーザＩＤ、マスタパスワード及びサブパスワードでネットワークにアクセスした履歴が一覧表示される。

【００３２】図８(ａ)は、全く異常アクセスが記録されなかった場合のアクセスログ表示を示す図であり、図８(ｂ)は、異常アクセスが記録された場合のアクセスログ表示を示す図である。このアクセスログファイルの一覧はログイン情報として表示される。開始における年月日及び時間が接続開始年月日及び接続開始時間である。終了における年月日及び時間が接続終了年月日及び接続終了時間である。接続時間は、接続終了時間から接続開始時間を(年月日を考慮して)減算した結果である。端末番号は、実際にネットワークに接続したクライアントの端末ＩＤである。図８(ｂ)のアスタリスク(＊)が表示された下のデータが異常アクセスを示している。すなわち、96-08-03及び96-08-04の開始時間２：４５及び２２：１７と、終了時間３：１２及び２：０３は、接続条件として登録された接続可能時間帯から外れているため、異常アクセスとして記録された。また、96-08-03及び96-08-04の両日の端末番号GHI54321は、接続条件として登録された端末ＩＤと一致しないために異常アクセスとして記録された。さらに、96-08-04の接続時間３時間４６分は、接続条件として登録された接続時間上限を越えているため異常アクセスとして記録された。

【００３３】このアクセスログ表示を見ることにより、ユーザ(操作者)はアスタリスクの有り無しを見て、そのアスタリスクの箇所を確認するだけで、簡単に不正アクセスを検出することができる。そして、この不正アクセスを行った者は、深夜時間に端末番号GHI54321のクライアント(クライアントマシン)を使用してアクセスした者であることまで判明する。ログイン(ネットワークへ接続)した後でも、接続時間が監視され、接続条件として登録された接続時間上限を越えたアクセスは異常アクセスとして記録し、強制ログオフが指定されている場合には、サーバ２は、強制的にそのクライアント３-xのネットワークへの接続を切断する。

【００３４】このようにこの実施の形態によれば、ネットワークを管理するサーバ２に各ユーザ毎に接続条件(接続時間上限、接続可能時間帯、接続可能曜日帯、接続回数上限及び接続端末ＩＤ)を登録したユーザ別情報ファイル１２と、各ユーザ毎にアクセスした接続状況を示すアクセスログファイルを履歴的に記憶するユーザ別アクセスログファイル１３とを設け、接続条件を満たさないアクセスについてはアクセスログファイルに異常アクセスを記録し、ログインしたクライアントに対して履歴的にアクセスログファイルを送信して表示させることにより、不正アクセスを防止すると共に検出することができ、不正アクセス検出におけるユーザの負担を軽減することができる。さらに、不正アクセスの内容すなわち接続時間及び接続端末ＩＤ等を知ることができ、不正アクセスを解決するための資料を供給することができる。

【００３５】なお、この実施の形態では、接続条件として、接続可能時間帯及び接続可能曜日帯を登録できるようになっていたが、この発明はこれに限定されるものでなく、例えば、毎月の特定な日(１日、１５日、２０日、２５日など)を指定できるもので良いし、平日に限定して指定できるものでも良いし、また逆に、土曜、日曜及び祭日に限定して指定できるものでも良いものである。

【００３６】

【発明の効果】以上詳述したようにこの発明によれば、不正アクセスを防止すると共に検出することができ、不正アクセス検出におけるユーザの負担を軽減することができるネットワークシステムを提供できる。

【図面の簡単な説明】

【図１】この発明の実施の形態のネットワークシステムの要部構成を示すブロック図。

【図２】同実施の形態のネットワークシステムのサーバの各クライアントに対するログオン及びログオフ制御に関する要部機能構成を示すブロック図。

【図３】同実施の形態のネットワークシステムのサーバのユーザ別情報ファイルのフォーマット例を示す図。

【図４】同実施の形態のネットワークシステムのサーバのユーザ別アクセスログファイルのフォーマット例を示す図。

【図５】同実施の形態のネットワークシステムの各クライアントがそれぞれ行うメイン処理の流れを示す図。

【図６】同実施の形態のネットワークシステムのサーバ

11

がログイン要求を受信したときに行うログイン処理の流れを示す図。

【図７】同実施の形態のネットワークシステムのサーバがネットワークに接続したクライアントに応対して定期的又はログオフ要求を受信した時に行うログオフ処理の流れを示す図。

【図８】同実施の形態のクライアントに表示されるアクセスログ表示の異常アクセスがないのときの一例及び異＊

12

＊常アクセスがある時の一例を示す図。

【符号の説明】

１…ネットワーク、

２…サーバ、

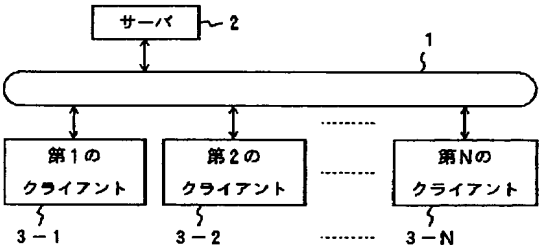
３-1～３-N

１１…中央制御部、

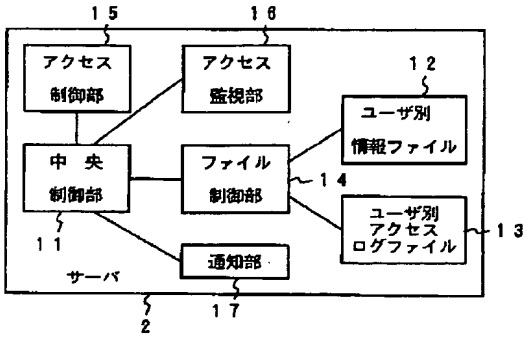
１２…ユーザ別情報ファイル、

１３…ユーザ別アクセスログファイル。

【図１】



【図２】



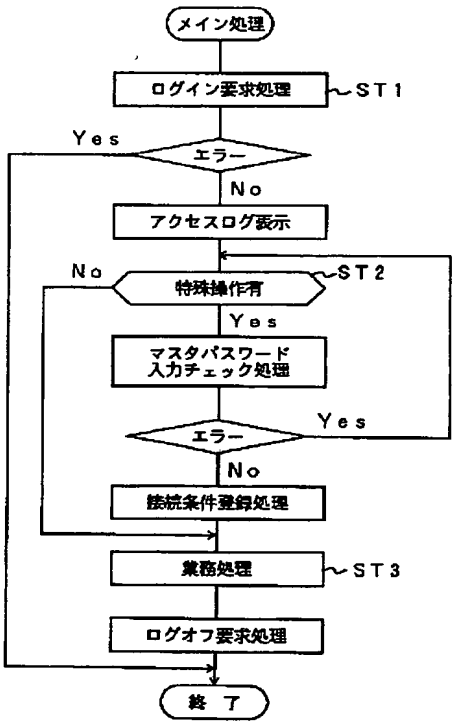
【図３】

ユーザＩＤ	
マスタパスワード	
サブパスワード	
接続条件	接続時間上限
	接続可能時間帯
	接続可能曜日帯
	接続回数上限
	接続端末ＩＤ
接続状況	接続開始年月日
	接続開始時間
	接続終了年月日
	接続終了時間
	接続回数

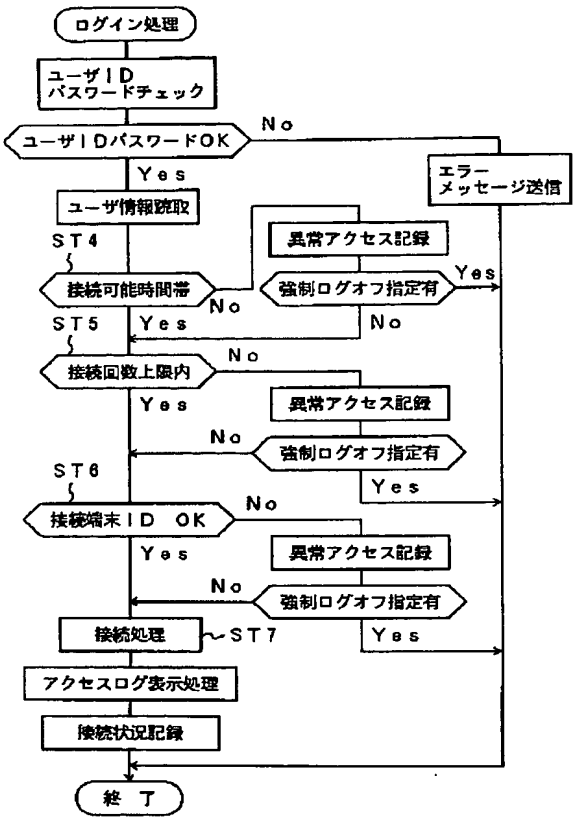
【図４】

ユーザＩＤ
接続開始年月日
接続開始時間
接続終了年月日
接続終了時間
接続時間
接続端末ＩＤ
アクセスステータス

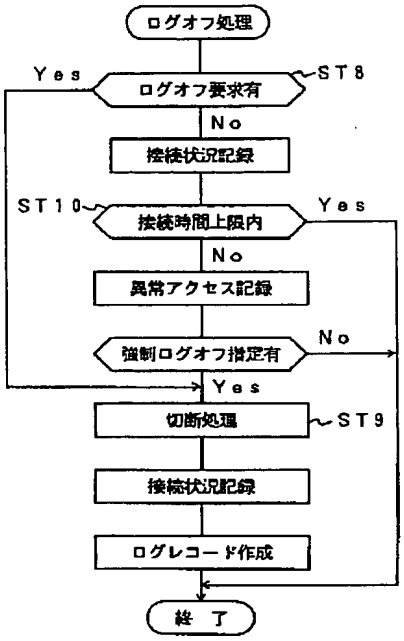
【図５】



【図６】



【図７】



【図８】

ログイン情報

開始 年月日	開始 時間	終了 年月日	終了 時間	接続時間	端末番号
96-08-01	15：40	96-08-01	16：29	59分	DEF67890
96-08-01	10：02	96-08-01	10：17	15分	ABC12345
96-08-01	8：23	96-08-01	8：55	32分	ABC12345
96-07-22	13：03	96-07-22	13：27	24分	ABC12345
96-07-18	9：20	96-07-18	9：53	33分	ABC12345

異常なアクセスは検出されていません。

(a)

ログイン情報

開始 年月日	開始 時間	終了 年月日	終了 時間	接続時間	端末番号
96-08-04	2：45	96-08-04	3：12	27分	GHI54321
96-08-03	22：17	96-08-04	2：03	3時間46分	GHI54321
96-08-01	15：40	96-08-01	16：29	59分	DEF67890
96-08-01	10：02	96-08-01	10：17	15分	ABC12345
96-08-01	8：23	96-08-01	8：55	32分	ABC12345
96-07-22	13：03	96-07-22	13：27	24分	ABC12345
96-07-18	9：20	96-07-18	9：53	33分	ABC12345

異常なアクセスが検出されました。

(b)